3621 EA

1 IFW

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/715,176	11/20/2000	Charles E. Sigler JR.	198966US-8	6429

7590 06/27/2005

eCogNito, Inc.
8619 Westwood Center Drive
Suite 420
Vienna, VA 22812

EXAMINER	
WORJLOH, JALATEE	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 06/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/715,176	SIGLER ET AL.	
	Examiner	Art Unit	
	Jalatee Worjloh	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 July 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-52* is/are pending in the application.

4a) Of the above claim(s) *15-23 and 52* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14,24 and 43-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *5-4-01, 1-22-01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1. Claims 15-23, 25-42 and 52 are withdrawn from further consideration pursuant to 37 CFR 1.142(b), as being drawn to a nonelected invention, there being no allowable generic or linking claim. Applicant timely traversed the restriction (election) requirement in the reply filed on 07/27/2004.

2. Applicant's election with traverse of claims 1-14, 24 and 43-51 in the reply filed on 07/27/2004 is acknowledged. The traversal is on the ground(s) that "the outstanding Restriction Requirement has not established that an undue burden would exist if the Restriction Requirement was not issued and all the claims were examined together". This is not found persuasive because Invention II and III utility such labeling/relabeling a parcel and determining a fraud score for a transaction, respectively. Because these invention are distinct for the reasons given above and the search required for Inventions II and II are not required for Invention I, restriction for examination purposes as indicated is proper.

The requirement is still deemed proper and is therefore made FINAL.

3. Claims 1-14, 24 and 43-51 have been examined.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1, 9 and 43 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are directed to a process that does nothing

more than manipulate an abstract idea. There is no practical application in the technological arts. All that is necessary to make a sequence of operational steps a statutory process within 35 U.S.C. 101 is that it be in the technological arts so as to be consonance with the Constitutional purpose to promote the progress of "useful arts." *In re Musgrave,* 431 F.2d 882, 167 USPQ 280 (CCPA 1970). Also, a claim is limited to a practical application when the method, as claimed, produces a concrete, tangible and useful result: i.e. the method recites a step or act of producing something that is concrete, tangible and useful. *See AT&T v. Excel Communications Inc.,* 172F.3d at 1358, 50 USPQ2dat 1452.

Claim Rejections - 35 USC § 103

5. Claims 1-14, 24 and 43-51 are rejected under 35 U.S.C. 103(a) as being unpatentable over "An Efficient Fair Payment System" to Camenisch et al. in view of US Publication No. 2004/0002903 to Stolfo et al.

Camenisch et al. disclose receiving by a trusted third party from the buyer and indicator of a payment method and assigning an anonymous identifier to the indicator that corresponds to the payment method (see pages 90 & 91, *Opening of a Personal Account, Registration at the Judge and Payment*). Camenisch et al. do not expressly disclose populating by the trusted third party a digital repository with data that is associated with the buyer, the data including a buyer identification indicator, the indicator of the payment method, and the anonymous identifier, purchasing by the buyer a product having a total sale price from a seller, providing by the buyer the anonymous identifier to the trusted third party as an anonymous payment method for the product, requesting by the seller payment approval by providing the total sale price to the trusted third party, querying by the trusted third party to determine the payment method from the

anonymous identifier received in the providing step, requesting by the trusted third party payment approval from a payment partner by providing the payment partner a description of the payment method determined in the querying step and the total sale price and providing payment approval to the seller. Stolfo et al. disclose populating by the trusted third party a digital repository with data that is associated with the buyer, the data including a buyer identification indicator, the indicator of the payment method, and the anonymous identifier (see paragraph [0051] Only the party providing the first party with the transacting identity can link the true identity of the first party with the transaction identity. Where a purchase is involved, the bank or credit clearing entity stores information linking the true identity of the user and the transaction identity. The bank or credit card clearing entity generates these transacting identities for all customers who use the inventive system and method, and provides a database linking the transacting and true identities.), purchasing by the buyer a product having a total sale price from a seller (see paragraph [0035]), providing by the buyer the anonymous identifier to the trusted third party as an anonymous payment method for the product (see paragraph [0127]), requesting by the seller payment approval by providing the total sale price to the trusted third party (see paragraph [0138] The proxy computer software waits for and receives from the second party vendor confirmation information that the proxy computer software stores for future reference. The information includes all identifying information transmitted to the second party vendor as well as typically complete list of items ordered from the second vendor.), querying by the trusted third party to determine the payment method from the anonymous identifier received in the providing step (see paragraphs [0140] - [0142] the proxy system passes to the bank the user's proxy identifier that allows the bank to identify the user as a bank customer and access the

customer's account. In an alternative embodiment, the proxy system database may store user bank account information linked to the proxy identifier, and the proxy system may transmit this account information), requesting by the trusted third party payment approval from a payment partner (i.e. other party) by providing the payment partner a description of the payment method determined in the querying step and the total sale price and providing payment approval to the seller (see paragraphs [0059] & [0060] Approval or disapproval may comprise another party providing for approval or disapproval of the purchase. The other party may be a third party who approves or disapproves of the purchase based on financial information relating to the first party and who also pays the second party and debits the first party if the purchase is approved. The other party may arrange with at least a third party to provide for approval or disapproval of the purchase.). The process of requesting by the trusted third approval form a payment partner is an inherent step. Notice, the "other party" informs the third party if the transaction is approve or deny, which implies that the third party must have first requested such authorization. At the time the invention was made, it would have been obvious to a person of ordinary skill the art to modify the method disclose by Camenisch et al to include the steps of populating by the trusted third party a digital repository with data that is associated with the buyer, the data including a buyer identification indicator, the indicator of the payment method, and the anonymous identifier, purchasing by the buyer a product having a total sale price from a seller, providing by the buyer the anonymous identifier to the trusted third party as an anonymous payment method for the product, requesting by the seller payment approval by providing the total sale price to the trusted third party, querying by the trusted third party to determine the payment method from the anonymous identifier received in the providing step, requesting by the trusted third party

payment approval from a payment partner by providing the payment partner a description of the payment method determined in the querying step and the total sale price and providing payment approval to the seller. One of ordinary skill in the art would have been motivated to do this because protects a purchaser's identity during electronic commerce transactions, thereby reducing fraudulent purchases (see Stolfo et al. paragraphs [0030]-[0032]).

Referring to claims 2,3, 44 and 45, Camenisch et al. disclose an anonymous payment method (see claim 1 above). Camenisch et al. do not expressly disclose the payment partner is a credit processor that receives credit approval from a credit approval authority or the payment partner is a credit approval authority. Stolfo et al. disclose the payment partner is a credit processor that receives credit approval from a credit approval authority or the payment partner is a credit approval authority (see paragraphs [0070], [0094] and [0143]). At the time the invention was made, it would have been obvious to a person of ordinary skill the art to modify the method disclose by Camenisch et al. to include the step wherein the payment partner is a credit processor that receives credit approval from a credit approval authority or the payment partner is a credit approval authority. One of ordinary skill in the art would have been motivated to do this because it provides an additional level of security.

Referring to claims 4 and 46, Camenisch et al. the payment method is at least one of a credit card, debit cad, an e-check, and a direct debit account (see pg. 91, *Withdrawal from Personal Account,* and *Payment*).

Referring to claims 5-7,10-12 and 47-49, Camenisch et al. disclose an anonymous payment method, wherein the anonymous identifier is a unique code (see pg. 90, anonymous account number *yA*). Camenisch et al. do not expressly disclose the anonymous identifier is

nickname or a one-time use code. Stolfo et al. disclose the anonymous identifier is nickname and a one-time use code (see paragraph [0047] the user has a different identity for each time it establishes communication with a second party or for each transaction [0048] the proxy can provide a user name which is a function of a unique name or proxy identifier of each user and the proxy's identity for each transaction). At the time the invention was made, it would have been obvious to a person of ordinary skill the art to modify the method disclose by Camenisch et al. to include the step wherein anonymous identifier is nickname or a one-time use code. One of ordinary skill in the art would have been motivated to do this because protects a purchaser's identity during electronic commerce transactions, thereby reducing fraudulent purchases (see Stolfo et al. paragraphs [0030]-[0032]).

Referring to claims 8 and 14, Camenisch et al. disclose the anonymous identifier is assigned by at least one of the buyer and the seller (see pg. 90, *Registration at the Judge,* the customer must first generate an new anonymous account number *yA*). At the time the invention was made, it would have been obvious to a person of ordinary skill the art to modify the method disclose by Camenisch et al. to include the step wherein the anonymous identifier is assigned by at least one of the buyer and the seller the. One of ordinary skill in the art would have been motivated to do this because protects a purchaser's identity during electronic commerce transactions, thereby reducing fraudulent purchases (see Stolfo et al. paragraphs [0030]-[0032]).

Referring to claim 9, Camenisch et al. disclose establishing by a trusted third party for a buyer a prefunded cash account, assigning an anonymous identifier to the prefunded account (see pages 90 & 91, *Opening of a Personal Account, Registration at the Judge, Opening of the Anonymous Account and Payment*). Camenisch et al. do not expressly disclose populating by the

trusted third party a digital repository with data that is descriptive of the buyer, the data including a buyer identification indicator, the identification indicator for the prefunded cash account and the anonymous identifier, purchasing by the buyer a product having a total sale price from a seller, providing by the buyer the anonymous identifier to the trusted third party as an anonymous payment method for the product, requesting by the seller payment approval by providing the total sale price to the trusted third party, querying by the trusted third party to determine the payment method from the anonymous identifier received in the providing step, requesting by the trusted third party payment approval from a payment partner by providing the payment partner a description of the payment method determined in the querying step and the total sale price and providing payment approval to the seller. Stolfo et al. populating by the trusted third party a digital repository with data that is descriptive of the buyer, the data including a buyer identification indicator, the identification indicator for the prefunded cash account and the anonymous identifier (see paragraph [0051] Only the party providing the first party with the transacting identity can link the true identity of the first party with the transaction identity. Where a purchase is involved, the bank or credit clearing entity stores information linking the true identity of the user and the transaction identity. The bank or credit card clearing entity generates these transacting identities for all customers who use the inventive system and method, and provides a database linking the transacting and true identities.), purchasing by the buyer a product having a total sale price from a seller (see paragraph [0035]), providing by the buyer the anonymous identifier to the trusted third party as an anonymous payment method for the product (see paragraph [0127]), requesting by the seller payment approval by providing the total sale price to the trusted third party (see paragraph [0138] The proxy computer software waits for and

receives from the second party vendor confirmation information that the proxy computer software stores for future reference. The information includes all identifying information transmitted to the second party vendor as well as typically complete list of items ordered from the second vendor.), querying by the trusted third party to determine the payment method from the anonymous identifier received in the providing step (see paragraphs [0140] - [0142] the proxy system passes to the bank the user's proxy identifier that allows the bank to identify the user as a bank customer and access the customer's account. In an alternative embodiment, the proxy system database may store user bank account information linked to the proxy identifier, and the proxy system may transmit this account information), requesting by the trusted third party payment approval from a payment partner (i.e. other party) by providing the payment partner a description of the payment method determined in the querying step and the total sale price and providing payment approval to the seller (see paragraphs [0059] & [0060]. Approval or disapproval may comprise another party providing for approval or disapproval of the purchase. The other party may be a third party who approves or disapproves of the purchase based on financial information relating to the first party and who also pays the second party and debits the first party if the purchase is approved. The other party may arrange with at least a third party to provide for approval or disapproval of the purchase.). The process of requesting by the trusted third approval form a payment partner is an inherent step. Notice, the "other party" informs the third party if the transaction is approve or deny, which implies that the third party must have first requested such authorization. At the time the invention was made, it would have been obvious to a person of ordinary skill the art to modify the method disclose by Camenisch et al to include the steps of populating by the trusted third party a digital repository with data that is associated with

the buyer, the data including a buyer identification indicator, the indicator of the payment method, and the anonymous identifier, purchasing by the buyer a product having a total sale price from a seller, providing by the buyer the anonymous identifier to the trusted third party as an anonymous payment method for the product, requesting by the seller payment approval by providing the total sale price to the trusted third party, querying by the trusted third party to determine the payment method from the anonymous identifier received in the providing step, requesting by the trusted third party payment approval from a payment partner by providing the payment partner a description of the payment method determined in the querying step and the total sale price and providing payment approval to the seller. One of ordinary skill in the art would have been motivated to do this because protects a purchaser's identity during electronic commerce transactions, thereby reducing fraudulent purchases (see Stolfo et al. paragraphs [0030]-[0032]).

Referring to claim 24, Camenisch et al. disclose means for (the judge's terminal) receiving by a trusted third party from the buyer and indicator of a payment method and means for (i.e. customer's device) assigning an anonymous identifier to the indicator that corresponds to the payment method (see pages 90 & 91, *Opening of a Personal Account, Registration at the Judge and Payment and pg. 93, Implementation*). Camenisch et al. do not expressly disclose means for populating by the trusted third party a digital repository with data that is associated with the buyer, the data including a buyer identification indicator, the indicator of the payment method, and the anonymous identifier, means for purchasing by the buyer a product having a total sale price from a seller, means for providing by the buyer the anonymous identifier to the trusted third party as an anonymous payment method for the product, means for requesting by

the seller payment approval by providing the total sale price to the trusted third party, means for querying by the trusted third party to determine the payment method from the anonymous identifier received in the providing step, means for requesting by the trusted third party payment approval from a payment partner by providing the payment partner a description of the payment method determined in the querying step and the total sale price and means for providing payment approval to the seller. Stolfo et al. disclose means for (i.e. database) populating by the trusted third party a digital repository with data that is associated with the buyer, the data including a buyer identification indicator, the indicator of the payment method, and the anonymous identifier (see paragraph [0051] Only the party providing the first party with the transacting identity can link the true identity of the first party with the transaction identity. Where a purchase is involved, the bank or credit clearing entity stores information linking the true identity of the user and the transaction identity. The bank or credit card clearing entity generates these transacting identities for all customers who use the inventive system and method, and provides a database linking the transacting and true identities.), means (i.e. computer, see paragraph [0045]) for: purchasing by the buyer a product having a total sale price from a seller (see paragraph [0035]), providing by the buyer the anonymous identifier to the trusted third party as an anonymous payment method for the product (see paragraph [0127]), requesting by the seller payment approval by providing the total sale price to the trusted third party (see paragraph [0138] The proxy computer software waits for and receives from the second party vendor confirmation information that the proxy computer software stores for future reference. The information includes all identifying information transmitted to the second party vendor as well as typically complete list of items ordered from the second vendor.), querying by the trusted third party to

determine the payment method from the anonymous identifier received in the providing step (see paragraphs [0140] - [0142] the proxy system passes to the bank the user's proxy identifier that allows the bank to identify the user as a bank customer and access the customer's account. In an alternative embodiment, the proxy system database may store user bank account information linked to the proxy identifier, and the proxy system may transmit this account information), requesting by the trusted third party payment approval from a payment partner (i.e. other party) by providing the payment partner a description of the payment method determined in the querying step and the total sale price and providing payment approval to the seller (see paragraphs [0059] & [0060] Approval or disapproval may comprise another party providing for approval or disapproval of the purchase. The other party may be a third party who approves or disapproves of the purchase based on financial information relating to the first party and who also pays the second party and debits the first party if the purchase is approved. The other party may arrange with at least a third party to provide for approval or disapproval of the purchase.). The process of requesting by the trusted third approval form a payment partner is an inherent step. Notice, the "other party" informs the third party if the transaction is approve or deny, which implies that the third party must have first requested such authorization. At the time the invention was made, it would have been obvious to a person of ordinary skill the art to system disclose by Camenisch et al to include means for: populating by the trusted third party a digital repository with data that is associated with the buyer, the data including a buyer identification indicator, the indicator of the payment method, and the anonymous identifier, purchasing by the buyer a product having a total sale price from a seller, providing by the buyer the anonymous identifier to the trusted third party as an anonymous payment method for the product, requesting

by the seller payment approval by providing the total sale price to the trusted third party, querying by the trusted third party to determine the payment method from the anonymous identifier received in the providing step, requesting by the trusted third party payment approval from a payment partner by providing the payment partner a description of the payment method determined in the querying step and the total sale price and providing payment approval to the seller. One of ordinary skill in the art would have been motivated to do this because protects a purchaser's identity during electronic commerce transactions, thereby reducing fraudulent purchases (see Stolfo et al. paragraphs [0030]-[0032]).

Referring to claims 43 and 51, Camenisch et al. disclose receiving by a trusted third party from the buyer and indicator of a payment method, assigning an anonymous identifier to the indicator that corresponds to the payment method and providing by the buyer to the trusted third party the anonymous identifier as an anonymous payment method for the product, wherein the anonymous identifier is assigned by at least one of the buyer and the trusted third party (see pages 90 & 91, *Opening of a Personal Account, Registration at the Judge and Payment*). Camenisch et al. do not expressly disclose assigning by the trusted third party at least one unique buyer-seller identifier, each corresponding to a unique combination of the buyer and at least one sellers, populating by the trusted third party a digital repository with data that is descriptive of the buyer, the data including a buyer identification indicator, the indicator of the payment method, and the anonymous identifier, and at least one unique buyer-seller identifier, purchasing by the buyer a product having a total sale price from a seller, providing by the buyer the an appropriate one of the at least one buyer-seller identifiers to the one of at least one sellers, the appropriate one of the at least one unique buyer-seller identifiers corresponding to the buyer and

the one of the at least seller, requesting by the seller payment approval by providing the total sale price to the trusted third party, querying by the trusted third party the digital repository to determine the payment method from the anonymous identifier received in the providing by the buyer to the trusted third party step, requesting by the trusted third party payment approval from a payment partner by providing the payment partner the payment method determined in the querying step and the total sale price, providing payment approval to the seller, requesting by the one of the at least sellers to the trusted third party a communication of a message to the buyer by providing the trusted third party the appropriate one of the at least one unique buyer-identifiers and forwarding by the trusted third party the message to the buyer by determining an identity of the buyer using the appropriate one of the at least one unique buyer-seller identifiers received in the requesting step. Stolfo et al. disclose assigning by the trusted third party at least one unique buyer-seller identifier, each corresponding to a unique combination of the buyer and at least on seller (see paragraph [0107] The unique transaction identifier serves to hid the true identity of the recipient and indexes the transaction. The unique transaction identifier may therefore serve as a data to the entire transaction any may be used to store and access transaction data such as recipient name, address, second party vendor.), populating by the trusted third party a digital repository with data that is associated with the buyer, the data including a buyer identification indicator, the indicator of the payment method, and the anonymous identifier and at east one unique buyer-seller identifier (see paragraph [0051] Only the party providing the first party with the transacting identity can link the true identity of the first party with the transaction identity. Where a purchase is involved, the bank or credit clearing entity stores information linking the true identity of the user and the transaction identity. The bank or credit card clearing entity

generates these transacting identities for all customers who use the inventive system and method, and provides a database linking the transacting and true identities.), providing by the buyer an appropriate one of the at least one unique buyer-seller identifiers to the one of the at least one sellers, the appropriate one of the at least one unique buyer-seller identifiers corresponding to the buyer and the one of the at least one seller (see paragraph [0107]; notice, "the unique transaction identifier may be linked to a tracking number", which implies that the buyer can provide it to the seller for tracking or other purposes), purchasing by the buyer a product having a total sale price from a seller (see paragraph [0035]), providing by the buyer the anonymous identifier to the trusted third party as an anonymous payment method for the product (see paragraph [0127]), requesting by the seller payment approval by providing the total sale price to the trusted third party (see paragraph [0138] The proxy computer software waits for and receives from the second party vendor confirmation information that the proxy computer software stores for future reference. The information includes all identifying information transmitted to the second party vendor as well as typically complete list of items ordered from the second vendor.), querying by the trusted third party to determine the payment method from the anonymous identifier received in the providing step (see paragraphs [0140] - [0142] the proxy system passes to the bank the user's proxy identifier that allows the bank to identify the user as a bank customer and access the customer's account. In an alternative embodiment, the proxy system database may store user bank account information linked to the proxy identifier, and the proxy system may transmit this account information), requesting by the trusted third party payment approval from a payment partner (i.e. other party) by providing the payment partner a description of the payment method determined in the querying step and the total sale price and providing payment approval to the

seller (see paragraphs [0059] & [0060] Approval or disapproval may comprise another party providing for approval or disapproval of the purchase. The other party may be a third party who approves or disapproves of the purchase based on financial information relating to the first party and who also pays the second party and debits the first party if the purchase is approved. The other party may arrange with at least a third party to provide for approval or disapproval of the purchase.). The process of requesting by the trusted third approval form a payment partner is an inherent step. Notice, the "other party" informs the third party if the transaction is approve or deny, which implies that the third party must have first requested such authorization. As for the steps of requesting by one of the at least one sellers to the trusted third party a communication of a message to the buyer by providing to the trusted third party the appropriate one of the at least one unique buyer-seller identifiers and forwarding the trusted third party the message to the buyer by determining an identity of the buyer using the appropriate one of the at least one unique buyer-seller identifiers received in the requesting step, Stolfo et al. provides a system to allows the buyer, seller and trusted third party to communicate messages (see paragraph [0045]). Stolfo et al. do not explicitly state that communication of the message includes providing one unique-buyer-seller identifies and using the buyer-seller identifiers received to forward the message. However, this is difference is found in the nonfunctional descriptive material and are not functionally involved in the steps recited. The requesting and forwarding steps would be performed the same regardless of the data. Thus, this descriptive material will not distinguish the claimed invention from the prior art in terms of patentability, *see In re Gulack,* 703F.2d 1381, 1385, 217 USPQ 401, 404 (Fed. Cir. 1983); *In re* Lowry, 32 F.3d 1579, 32 USPQ2d 1031 (Fed. Cir. 1994). At the time the invention was made, it would have been obvious to a person of

ordinary skill the art to modify the method disclose by Camenisch et al to include the steps of assigning by the trusted third party at least one unique buyer-seller identifier, each corresponding to a unique combination of the buyer and at least one sellers, populating by the trusted third party a digital repository with data that is descriptive of the buyer, the data including a buyer identification indicator, the indicator of the payment method, and the anonymous identifier, and at least one unique buyer-seller identifier, purchasing by the buyer a product having a total sale price from a seller, providing by the buyer the an appropriate one of the at least one buyer-seller identifiers to the one of at least one sellers, the appropriate one of the at least one unique buyer-seller identifiers corresponding to the buyer and the one of the at least seller, requesting by the seller payment approval by providing the total sale price to the trusted third party, querying by the trusted third party the digital repository to determine the payment method from the anonymous identifier received in the providing by the buyer to the trusted third party step, requesting by the trusted third party payment approval from a payment partner by providing the payment partner the payment method determined in the querying step and the total sale price, providing payment approval to the seller, requesting by the one of the at least sellers to the trusted third party a communication of a message to the buyer by providing the trusted third party the appropriate one of the at least one unique buyer-identifiers and forwarding by the trusted third party the message to the buyer by determining an identity of the buyer using the appropriate one of the at least one unique buyer-seller identifiers received in the requesting step. One of ordinary skill in the art would have been motivated to do this because protects a purchaser's identity during electronic commerce transactions, thereby reducing fraudulent purchases (see Stolfo et al. paragraphs [0030]-[0032]).

Referring to claim 51, Camenisch et al. disclose a method maintaining anonymity of a buyer and receiving proxy information from a buyer (see claim 43 above). Camenisch et al. do not expressly disclose receiving by the trusted third party an e-mail address for use in an anonymous communications with the at least one sellers, wherein the populating step comprises populating the digital repository with the e-mail address, and the message forwarded to the buyer is an e-mail message sent to the e-mail address. Stolfo et al. disclose receiving by the trusted third party an e-mail address (i.e. electronic address) for use in an anonymous communications with the at least one sellers (see paragraph [0057]), wherein the populating step comprises populating the digital repository with the e-mail address (see paragraph [0051] Where a purchase is involved, the bank or credit clearing entity stores information linking the true identity of the user.), and the message forwarded to the buyer is an e-mail message sent to the e-mail address (see paragraph [0150] the communications between the first party users and the proxy computer can be by e-mail).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jalatee Worjloh whose telephone number is (571)272-6714. The examiner can normally be reached on Mondays-Thursdays 8:30 - 7:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on (571)272-6712. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306 for Regular/After Final Actions and (571)273-6714 for Non-Official/Draft.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600

Jalatee Worjloh
Patent Examiner
Art Unit 3621

***

June 16, 2005

Form PTO 1449 (Modified) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTY DOCKET NO. 198966US8	SERIAL NO. 09/715,176
LIST OF REFERENCES CITED BY APPLICANT	APPLICANT Charles E. SIGLER, JR., et al.	
	FILING DATE November 20, 2000	GROUP 2165

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUB CLASS	FILING DATE IF APPROPRIATE
	AA	6,029,150	2/22/2000	D.W. KRAVITZ			
	AB	6,076,078	06/13/2000	L.J. CAMP, et al.			
	AC	6,138,107	10/24/2000	T. ELGAMAL			
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						
	AL						
	AM						
	AN						

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	TRANSLATION YES	TRANSLATION NO
	~~AO~~	~~10-187830~~	~~07/21/98~~	~~JAPAN (with English Abstract)~~		~~X~~
	AP					
	AQ					
	AR					
	AS					
	AT					
	AU					
	AV					

OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, etc.)

	AW	M. HODGES, MIT's Technology Review, Vol. 100, No. 6, pps. 26-27, "BUILDING A BOND OF TRUST," August/September 1997 (Filing edited pages 1-2 only)
	AX	B. JORGENSEN, Electronic Business, Vol. 26, No. 10, p. 41 +, "BUSINESS TRENDS (SOME $13.9 BIL OF ELECTRONICS PRODUCTS WILL BE SOLD THROUGH B2B E-MARKETPLACES IN 2000)", October 2000 (Filing edited pages 1-4 only)
	AY	
	AZ	

Examiner [signature] Date Considered 6-15-03

*Examiner: Initial if reference is considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form PTO 1449 (Modified)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTY DOCKET NO. 198966US-8	SERIAL NO. 09/715,176
LIST OF REFERENCES CITED BY APPLICANT		APPLICANT Charles E. SIGLER, JR., et al.	
		FILING DATE November 20, 2000	GROUP

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUB CLASS	FILING DATE IF APPROPRIATE
✓	AA	6,006,200	12-21-99	Boles, et al.			
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						
	AL						
	AM						
	AN						

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	TRANSLATION YES	TRANSLATION NO
	AO					
	AP					
	AQ					
	AR					
	AS					
	AT					
	AU					
	AV					

OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, etc.)

	AW	
	AX	
	AY	
	AZ	

Examiner [signature] Date Considered 6-15-05

*Examiner: Initial if reference is considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

BDL:TJF:fbl
I:\atty\tjf\10612 - eCogNito\198966\ids.1449.wpd

Notice of References Cited	Application/Control No. 09/715,176	Applicant(s)/Patent Under Reexamination SIGLER ET AL.	
	Examiner Jalatee Worjloh	Art Unit 3621	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-2004/0002903	01-2004	Stolfo et al.	705/26
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Camenisch et al., "An Efficient Fair Payment System", 1996, ACM
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

An Efficient Fair Payment System

Jan Camenisch*
Dept. of Computer Science
Haldeneggsteig 4
ETH Zürich
CH-8092 Zürich, Switzerland
Email: camenisch@inf.ethz.ch

Jean-Marc Piveteau
Union Bank of Switzerland
UBILAB
Bahnhofstrasse 45
CH-8021 Zürich, Switzerland
Email: piveteau@ubilab.ubs.ch

Markus Stadler*
Dept. of Computer Science
Haldeneggsteig 4
ETH Zürich
CH-8092 Zürich, Switzerland
Email: stadler@inf.ethz.ch

Abstract

Many proposed payment systems allow the payer to remain anonymous during a transaction. However, this unconditional privacy protection could be misused by criminals, e.g. for blackmailing or money laundering. With a fair payment system, anonymous payments are still possible, but the anonymity can be removed with the help of a trusted party which need not be involved in the transaction itself. In this paper, we present an efficient fair payment system and we discuss its security.

1 Introduction

Efficient electronic payment systems are an important prerequisite for electronic commerce. The design of such payment systems poses many security-related problems. Apart from the common security requirements such as the prevention of frauds, the protection of the participants' privacy is an important issue.

In many systems the protection of the user's privacy relies exclusively on administrative and legal measures. Using cryptographic tools such as blind signatures [7], it is possible to design electronic payment systems that allow participants to remain anonymous during a transaction, without affecting the security of the system (e.g. [2, 5, 8, 9]). Such systems offer an unconditional privacy protection, but they can be misused by criminals for perfect blackmailing [17] or for money laundering.

The concept of a *fair payment system*, independently proposed in [3] and [16], offers a compromise between the legitimate need of privacy protection and an effective prevention of misuse by criminals. On one hand, the customer's privacy cannot be compromised by the bank or by the payee. On the other hand, there is a trusted third party, called the judge, which can (in cooperation with the bank) remove the anonymity of a transaction if the system is being misused by criminals. Furthermore, the trusted third party is not involved in the transactions.

In this paper, we present an efficient fair payment system based on the anonymous payment system described in [5]. The system is currently realized as a prototype, with the customer functionality implemented on smart-cards.

The basic concepts of fair payment systems are discussed in Section 2. The new system is described in Section 3, followed by a discussion on its security. Some results on the prototype implementation are given in Section 4. Finally, in Section 5 we compare our proposal with other existing payment systems with similar properties.

2 Basic Concepts

An electronic payment system consists of a set of protocols between three interacting parties: a bank, a customer (the payer), and a shop (the payee). The customer and the shop have both an account with the bank. The goal of the system is to transfer money in a secure way from the customer's account to the shop's account. It is possible to identify three different phases: a *withdrawal phase* involving the bank and the customer, a *payment phase* involving the customer and the shop, and a *deposit phase* involving the shop and the bank. In an *off-line* system, each phase occurs in a separate transaction, whereas in an *on-line* system, such as ours, payment and deposit take place in a single transaction involving all three parties.

Bank, shop and customer have different security requirements. The bank wants to make sure that for each account credited, another account has been debited. The shop, receiving a payment, wants to be assured that the bank will accept to credit its account with the received amount. Finally, the customer wants to be sure that money he[1] has withdrawn will be accepted for a payment. Furthermore, the customer may require that his privacy be protected.

Anonymous electronic payment systems (e.g. [2, 5, 8, 9]) prevent anybody, including the bank, from violating the customer's privacy. Payments are anonymous and different payments of the same customer are unlinkable. This is achieved using cryptographic mechanisms such as blind signature schemes [4, 7].

*Supported by the Swiss Federal Commission for the Advancement of Scientific Research (KWF) and by the Union Bank of Switzerland.

CCS '96, New Delhi, India
© 1996 ACM 0-89791-829-0/96/03..$3.50

[1] In this paper the customer is male whereas the judge is female.

A problem with anonymous payment systems is that they could be misused by criminals, e.g. for perfect blackmailing [17] or for money laundering. This is possible because the anonymity of payments prevents the bank from tracing money.

Different measures have been proposed to offer a limited protection against this kind of threat. A restriction of the maximal possible amount transferred during a transaction should make the system unattractive for money laundering. However, this is effective only if the number of transactions that can be done during a short period of time is limited. In the case of blackmailing, a possible measure for systems such as [8] would be to stop the system when a withdrawal is done under threat, which is unrealistic.

The concept of *fair payment systems*[2] was independently proposed in [3] and [16]. A fair payment system, like other anonymous payment systems, protects the privacy of the customer. But in contrast to payment systems that protect the privacy unconditionally, there is an additional, trusted party, called the *judge*. The judge has the following attributes:

- She can remove the anonymity of a transaction in cooperation with the bank. This can happen in two different ways: Either the bank provides the judge with the data of a (suspect) withdrawal and asks for information that allows to identify the corresponding deposit (or payment), or the bank provides her with data of a (suspect) deposit and asks for the corresponding withdrawal.
- She is only involved during the setup of the system, possibly in the opening of accounts, but not in the transactions.
- She is trusted only in privacy-related matters, e.g. the bank may not trust her about forging money.

Note that it is possible to share the functionality of the judge among several trusted parties (e.g. the trustees in [3]).

An adequate protection against money laundering is offered by fair payment systems because it is possible for the judge, in cooperation with the bank, to determine the origin or the destination of dubious money transfers.

Fair payment systems also prevent the "perfect crime" scenario described in [17], where a customer is blackmailed and forced to act as an intermediary between the blackmailer and the bank during the withdrawal of money. In a perfectly anonymous payment system, the ransom cannot be recognized later. However, in a fair payment system, the judge can trace the blackmailed money.

3 Description of the Payment System

The fair payment system presented in this section is based on the anonymous payment system of [5]. Let us briefly recall its principle. The bank manages two types of accounts: *personal accounts*, of which the owner is known to the bank, and *anonymous accounts*, of which only a pseudonym of the owner is known. An anonymous payment is simply a transfer from a customer's anonymous account to the shop's account. The main part of the system consists of an efficient method for transferring money from a personal account to an anonymous account without revealing the correspondence between them. This is realized using an electronic coin that can be paid only into a single anonymous account. Therefore double-spending of the coin can be prevented by a simple counter (instead of maintaining a large database containing all spent coins). Furthermore, the perfect unlinkability of personal and anonymous accounts is realized by using a blind signature scheme. In order to achieve *fairness*, this system is modified in the following way:

- The judge knows the correspondence between personal and anonymous accounts.
- A coin withdrawn from a personal account can only be deposited into a corresponding (i.e. registered) anonymous account.

The basic idea of the fair payment system presented in this paper can be informally described as follows. A public key is associated with each personal account. To open a new anonymous account, the customer has to provide a public key which is derived from the public key of his personal account. The correspondence between the two keys must be registered at the judge. When actually opening the anonymous account, the bank checks whether this registration has taken place and whether the public key of the anonymous account is correctly constructed.

Coins withdrawn from the personal account are signed by the bank with respect to the public key of the personal account. The customer can then derive a valid signature with respect to the public key of a corresponding anonymous account. Signatures valid for other anonymous accounts cannot be derived.

Because of the registration of corresponding public keys, it is possible to trace transactions in cases of money laundering. Furthermore, tracing is also possible if the customer is blackmailed: coins can be paid only into an anonymous account that corresponds to the customer's personal account (even if the blackmailer opens the anonymous account himself).

3.1 Protocols

We now give a detailed description of the system. The initialization of the system is divided into three different steps: the *Opening of a Personal Account* (Fig. 1), the *Registration at the Judge* (Fig. 2), and the *Opening of an Anonymous Account* (Fig. 3).

After the initialization has been completed, money can be transferred from a personal account to a corresponding anonymous account. This transfer is split into two steps. During the *Withdrawal from Personal Account* (Fig. 4), the customer debits his personal account. The withdrawn money is paid into the corresponding anonymous account using the protocol *Deposit into Anonymous Account* (Fig. 5). A payment to a shop is made as a simple transfer from the customer's anonymous account to the shop's account.

Most of the described protocols need a preceding mutual identification of the involved parties by some adequate protocol. However, in some of the protocols the customer must not

[2]The terminology *fair payment system* has been actually introduced in [6]. It corresponds to the concept of payment systems with *trustee-based tracing* introduced in [3].

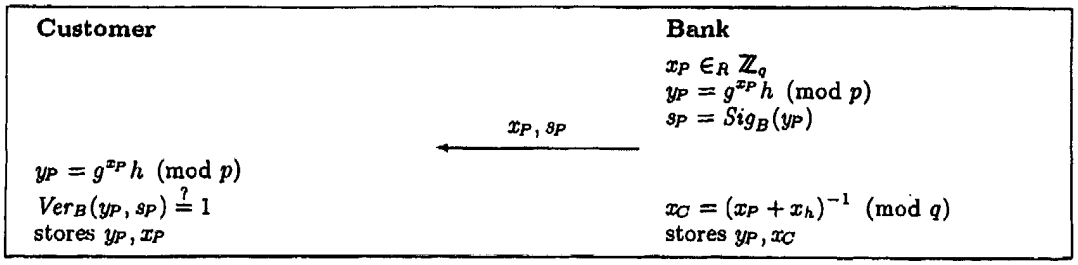

Figure 1: Opening of a Personal Account

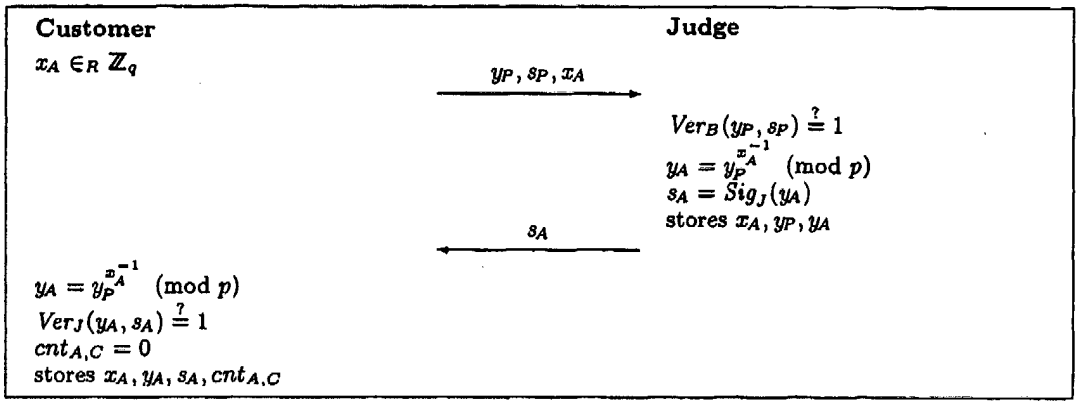

Figure 2: Registration at the Judge

be identified, i.e. the *Registration at the Judge*, the *Opening of the Anonymous Account*, and the *Deposit into Anonymous Account*.

System parameters

Let p be a large prime, q a prime divisor of $p-1$, $g \in \mathbb{Z}_p^*$ of multiplicative order q, and $\mathcal{H}$ a one-way hash function. The computation of the discrete logarithm modulo p to the base g is assumed to be intractable. Let V be the set of possible transaction values.The bank selects $x_h \in \mathbb{Z}_q$, and $x_v \in \mathbb{Z}_q$ for each $v \in V$. The values $g, h = g^{x_h} \pmod p$ and $\{z_v\}_{v \in V}$ with $z_v = g^{x_v} \pmod p$ are public, while x_h and $\{x_v\}_{v \in V}$ are kept secret. Let (Sig_B, Ver_B) be a signature scheme of the bank. Sig_B is the bank's secret signature generation function and Ver_B is the public verification function. The following must hold: $\forall m, s : Ver_B(m, s) = 1 \iff s = Sig_B(m)$. Similarly, let (Sig_J, Ver_J) be a signature scheme of the judge.

The concatenation of the strings α and β is denoted by $\alpha \| \beta$. The expression $\xi \in_R X$ means that ξ is randomly chosen from the (finite) set X according to the uniform distribution.

Opening of a Personal Account

First, the customer identifies himself to the bank. Then the protocol in Figure 1 is carried out. The bank chooses x_P at random, calculates y_P and sends x_P and a signature of y_P to the customer. The public key y_P can be considered as the account number of the personal account. The integer x_P can be seen as the customer's part of the secret key of y_P while x_C is the bank's part of this secret key.

Registration at the Judge

In order to open a new anonymous account, the customer must first generate a new anonymous account number y_A and register the correspondence between y_A and his personal account number y_P at the judge. This is accomplished by the protocol given in Figure 2. The customer chooses x_A at random and sends it together with y_P and s_P to the judge. By checking the bank's signature s_P the judge verifies that y_P is a valid account number. After having calculated y_A the judge sends the customer her signature of it. This signature now enables the customer to open the anonymous account. The variable $cnt_{A,C}$ is the customer's counter for the number of transfers between the accounts y_P and y_A.

Opening of the Anonymous Account

To open the anonymous account corresponding to y_A the customer contacts the bank anonymously. Then the protocol in Figure 3 is carried out. This protocol is essentially a proof by the customer to the bank that he knows the representation of y_A with respect to g and h, i.e. that he knows $\xi_1, \xi_2 \in \mathbb{Z}_q$ with $y_A = g^{\xi_1} h^{\xi_2}$ (see [1], section 8). By checking the validity of s_A, the bank verifies indirectly that the judge knows the personal account number corresponding to

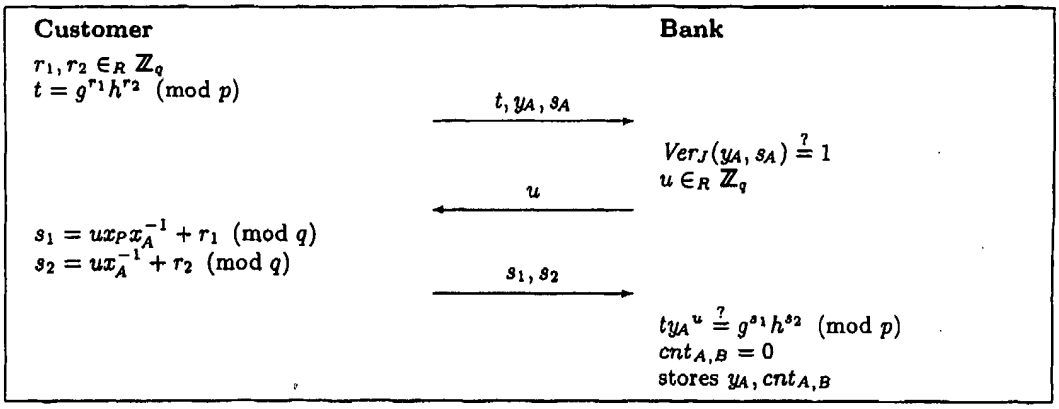

Figure 3: Opening of the Anonymous Account

y_A and vice versa. The variable $cnt_{A,B}$ is the bank's counter for the number of deposits into the anonymous account y_A. The customer does no longer need to store s_A at the end of this step.

Bank and customer also agree on some form of future authentication for the customer as the owner of this anonymous account.

Withdrawal from Personal Account

After having opened the anonymous account y_A the customer can transfer money to it. To do so he first withdraws money from his personal account y_P. After he is identified by the bank as the owner of the account, bank and customer execute the protocol as indicated in Figure 4. It is a protocol to blindly obtain a Schnorr-signature [15] (s', c) of the message $y_A \| cnt_{A,C}$ for the public key z_v with respect to the base y_P. Before the customer can pay the withdrawn money into his anonymous account, he must transform the obtained signature into one with respect to the base y_A. This can be done by simply multiplying s' by x_A. Thus the pair (s, c) is the signature of the message $y_A \| cnt_{A,C}$ for the public key z_v with respect to the base y_A. The corresponding verification equation is:

$$c = \mathcal{H}(t \| y_A \| cnt_{A,C})$$

where $t = y_A^s z_v^c \pmod p$.

Deposit into Anonymous Account

The protocol given in Figure 5 allows the customer to deposit the withdrawn money into the appropriate anonymous account. For this protocol there is no need for the bank to identify the customer.

Payment

When the money has been paid into the anonymous account, the customer can use it for a payment. For such a payment, the shop, the customer and the bank have to be on-line. The customer is identified by the bank as the owner of the anonymous account y_A. The payment itself is then a on-line transaction from account y_A to the shop's account. The bank only has to prevent overdraft, i.e. to check on-line the balance of the account used for the payment.

Although the customer's identity is not revealed, the bank can still link different transactions when the same anonymous account is used for different payments. However, for transactions that should not be linked by the bank, the customer can use different anonymous accounts corresponding to the same personal account.

Removal of the Anonymity

Since the judge knows the correspondence between personal and anonymous accounts, she can at any time find the origin or the destination of a transfer, when provided with anonymous or personal account numbers.

3.2 Security Analysis

Signature generated during the withdrawal protocol

The bank wants to be sure that the customer, even with the help of the judge, is not able to compute a valid coin without carrying out the withdrawal protocol. It appears to be practically impossible for the customer to generate a valid signature without knowing the discrete logarithm of z_v to the base y_A. In particular, it is easy to see that breaking the withdrawal protocol would imply that Okamoto's blind version [13] of Schnorr's scheme is insecure.

Furthermore, it is easy to see that the customer cannot compute the discrete logarithm of z_v to the base y_A, even in collaboration with the judge. The customer has indeed proved during the opening of the anonymous account that he knows ξ_1 and ξ_2 with $y_A = g^{\xi_1} h^{\xi_2} \pmod p$. Assume furthermore that he can determine the discrete logarithm of z_v to the base y_A. This means that he has an algorithm allowing, on input g, h, z_v, to compute ξ_1, ξ_2, ξ_A, y_A with $y_A = g^{\xi_1} h^{\xi_2} \pmod p$ and $z_v = y_A^{\xi_A} \pmod p$. This implies that, for given g, h, z_v, he has a procedure to find $\xi_1, \xi_2, \xi_3 \in \mathbb{Z}_q^*$ with $1 = g^{\xi_1} h^{\xi_2} z_v^{\xi_3} \pmod p$. However, the existence of such a procedure is known to be equivalent to the existence of an algorithm solving the discrete logarithm problem [1].

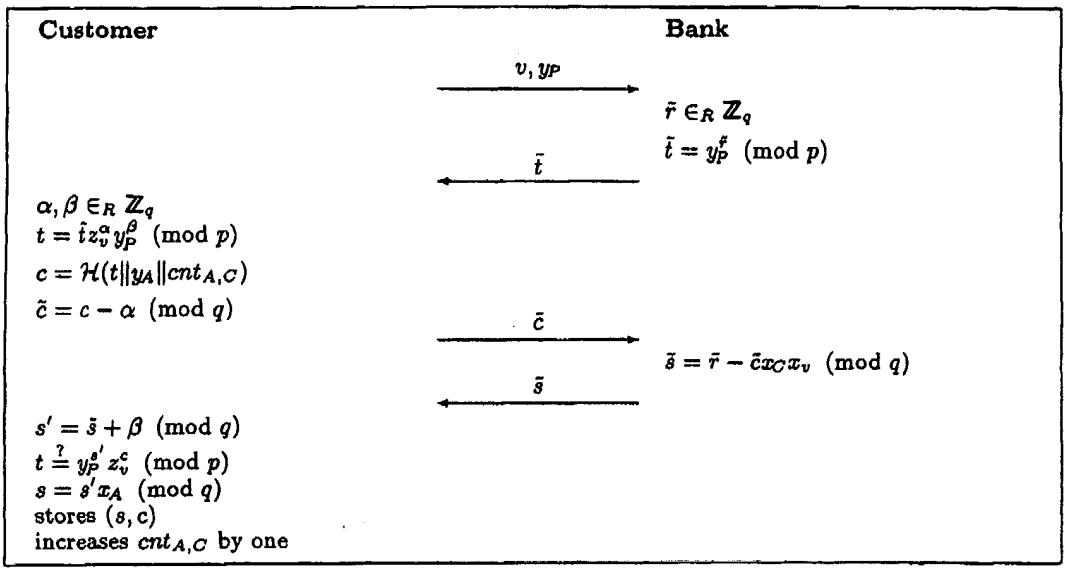

Figure 4: Withdrawal from Personal Account

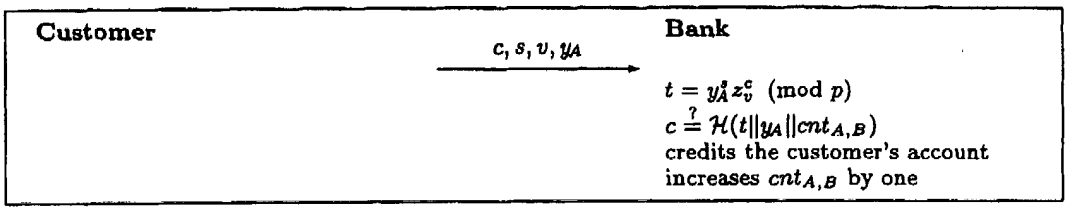

Figure 5: Deposit into Anonymous Account

Multiple payments

Because the electronic coin contains the anonymous account number, the customer cannot pay the same coin into different anonymous accounts. The counters cnt_{AC} and cnt_{AB} guarantee that the customer cannot deposit the same coin more than once into the same account.

Modification of the transfer value

The system should prevent a dishonest customer from withdrawing an electronic coin of value v and transforming it into a coin of value $v' > v$. This would be possible if the customer was able to compute the discrete logarithm of $z_{v'}$ to the base z_v; however, this is assumed to be an intractable problem. There seems to be no other way to modify the value of a given electronic coin.

Unlinkability of withdrawal and deposit

Obviously, unlinkability between the withdrawal from the personal account and the deposit into the anonymous account can be achieved only if many transactions (of each transaction value) take place. Additionally, the following has to be satisfied: First, it must not be possible for the bank to link transactions by analyzing the time they have taken place. Therefore, the customer should choose the period of time between withdrawal and deposit appropriately. Second, the bank's view of two corresponding transactions must be unlinkable. This is fulfilled because for each $v \in V$, the random variables $View_1^v = (x_C, y_P, \tilde{r}, \tilde{t}, \tilde{c}, \tilde{s})$ and $View_2^v = (y_A, s, c, cnt_{A,B})$ are statistically independent: For a given pair $(View_1^v, View_2^v)$, let x_A be the discrete logarithm of y_A to the base y_P, $\alpha = c - \tilde{c} \pmod q$ and $\beta = s x_A^{-1} - \tilde{s} \pmod q$. It is easy to see that this is the only possible choice for α and β if $View_1^v$ has to be the bank's view during the withdrawal phase corresponding to the deposit with bank's view given by $View_2^v$. It remains to show that this choice is always valid, i.e. that we have $c = \mathcal{H}(t \| y_A \| cnt_{A,B})$ where $t = \tilde{t} z_v^{\alpha} y_P^{\beta} \pmod p$. The following equalities are easy to check:

$$\begin{aligned}
\tilde{t}\, z_v^{\alpha} y_P^{\beta} &= y_P^{\tilde{r}}\, z_v^{c-\tilde{c}} y_P^{s x_A^{-1} - \tilde{s}} && \pmod p \\
&= y_P^{\tilde{r} - (\tilde{r} - \tilde{c} x_C x_v)} z_v^{c-\tilde{c}} y_P^{s x_A^{-1}} && \pmod p \\
&= y_P^{\tilde{c} x_C x_v} z_v^{c-\tilde{c}} y_A^{s} && \pmod p \\
&= z_v^{\tilde{c}} z_v^{c-\tilde{c}} y_A^{s} && \pmod p \\
&= y_A^{s} z_v^{c} && \pmod p
\end{aligned}$$

and therefore:

$$\mathcal{H}(t\|y_A\|cnt_{A,B}) = \mathcal{H}(y_A^s z_v^c \pmod p)\|y_A\|cnt_{A,B}) = c.$$

The last equality follows from the fact that (c, s) is a valid signature.

Cross-payments

A cross-payment is a transfer from a personal account y_P to an anonymous account $\tilde{y}_A$ which is registered at the judge to belong to another personal account $\tilde{y}_P$. To do such a cross-payment, it seems necessary that an attacker knows the discrete logarithm of $\tilde{y}_P$ to the base y_P, which would imply that he knows the secret value $x_h = \log_g h$. But this is assumed to be intractable and so cross-payments are not possible.

4 Implementation

It is essential for the customer that his private data (e.g. identification information, or secrete encryption key) are securely stored and not endangered when carrying out a protocol. This becomes even more important if the customer wants to be mobile and have access to the network at any point, even through untrusted terminals (e.g. shop's terminal). To fulfill these requirements, the customer needs a portable secure computing device such as a smart-card. This device is limited in size, thus its computation power and storage capacity are restricted.

To demonstrate the practicability and efficiency of the fair payment system described in this article, we decided to implement the customer's functionality on a smart-card (the Philips Cryptocard [14] with the 83C852-chip[3]). To simulate a real payment system environment, the implementation includes a key management, a mutual authentication procedure, and an encryption mechanism (based on the cipher IDEA [11]). The implementation allows the customer to manage one personal and two anonymous accounts on the card.

5 Related Work

There exist several other proposals for payment systems offering a conditional privacy protection [6, 3, 12] with a trusted third party.

In the anonymous credit card system [12] each customer is provided with a personal account and an anonymous account on another (Swiss) bank. Anonymous transfers between these two accounts are realized using an intermediary, called communication exchange. The information needed to link personal and anonymous accounts is shared among the customer's banks and the communication exchange, i.e. the banks have to cooperate with the communication exchange to recover this correspondence.

The first fair payment systems with an "off-line" trusted party have been proposed in [3], where unconditionally anonymous payment systems [2, 10] are extended by the concept of trustee-based tracing.

[3] 8-bit CPU (Intel 8051 family), 6 kByte ROM, 256 Byte RAM, 2 kByte EEPROM, 1-6 MHz clock frequency.

Independently, [16] described the concept of fair blind signature schemes, which allows a trusted third party to link a signed message to the corresponding signature generation and vice versa. By replacing the signature scheme it is possible transform unconditionally anonymous payment systems into fair payment systems. In [6] two variations of this method are described.

6 Conclusion

We have presented a new fair payment system. It allows customers to perform anonymous payments. However the anonymity can be removed on request by a trusted party. We believe that this approach offers a acceptable compromise between the legitimate right for privacy protection and the need for effective methods to prevent criminal misuses of this privacy. Furthermore, the efficiency of our proposal makes is well suited as a payment system over networks such as Internet and for implementations on smart cards.

Acknowledgments

The authors thank Ueli Maurer and H.-P. Frei for their support. Roberto Citrini, Markus Isler, Arthur Marxer and Martin Perewusnyk implemented the prototype. We are grateful for the help of Moti Yung in preparing this paper. Also the comments of the anonymous referees were much appreciated.

References

[1] S. Brands. An efficient off-line electronic cash system based on the representation problem. Technical Report CS-R9323, CWI, Apr. 1993.

[2] S. Brands. Electronic cash systems based on the representation problem in groups of prime order. In *Advances in Cryptology - CRYPTO '93*, volume 773 of *Lecture Notes in Computer Science*, pages 302–318. Springer Verlag, 1994.

[3] E. Brickell, P. Gemmel, and D. Kravitz. Trustee-based tracing extensions to anonymous cash and the making of anonymous change. In *Proceedings of the 6th Annual Symposium on Discrete Algorithms*, pages pp 457– 466, Jan. 1995.

[4] J. Camenisch, J.-M. Piveteau, and M. Stadler. Blind signatures based on the discrete logaritm problem. In A. D. Santis, editor, *Advances in Cryptology- EUROCRYPT '94*, volume 950 of *Lecture Notes in Computer Science*, pages 428–432. Springer Verlag Berlin, 1994.

[5] J. Camenisch, J.-M. Piveteau, and M. Stadler. An efficient payment system protecting privacy. In *Computer Security - ESORICS 94*, volume 875 of *Lecture Notes in Computer Science*, pages 207–215. Springer Verlag, 1994.

[6] J. Camenisch, J.-M. Piveteau, and M. Stadler. Faire Anonyme Zahlungssysteme. In F. Huber-Wäschle,

H. Schauer, and P. Widmayer, editors, *GISI 95*, Informatik aktuell, pages 254–265. Springer Verlag Berlin, Sept. 1995.

[7] D. Chaum. Blind signature systems. In D. Chaum, editor, *Advances in Cryptology - CRYPTO '83*, page 153. Plenum, 1983.

[8] D. Chaum. Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10):1030– 1044, Oct. 1985.

[9] D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In S. Goldwasser, editor, *Advances in Cryptology - CRYPTO '88*, volume 403 of *Lecture Notes in Computer Science*, pages 319–327. Springer Verlag, 1990.

[10] M. Franklin and M. Yung. Towards provably secure efficient electronic cash. Technical Report TR CUSC-018-92, Columbia University, Dept. of Computer Science, Apr. 1992. Also in: Proceedings of ICALP 93, Lund, Sweden, July 1993, volume 700 of LNCS, Springer Verlag.

[11] X. Lai. *On the Design and Security of Block Ciphers*, volume 1 of *ETH Series in Information Processing*. Hartung-Gorre Verlag Konstanz, 1992.

[12] S. H. Low, N. F. Maxemchuk, and S. Paul. Anonymous credit cards. In *2nd ACM Conference on Computer and Communication Security*, pages 108–117. acm press, Nov. 1994.

[13] T. Okamoto. Provable secure and practical identification schemes and corresponding signature schemes. In E. F. Brickell, editor, *Advances in Cryptology — CRYPTO '92*, volume 740 of *Lecture Notes in Computer Science*, pages 31–53. Springer-Verlag, 1993.

[14] Philips Semiconductor Hamburg- SCM. *83C852, Secured 8-bit microcontroller*, Sept. 1991. Data-Sheet.

[15] C. P. Schnorr. Efficient signature generation for smart cards. *Journal of Cryptology*, 4(3):239–252, 1991.

[16] M. Stadler, J.-M. Piveteau, and J. Camenisch. Fair blind signatures. In L. C. Guillou and J.-J. Quisquater, editors, *Advances in Cryptology - EUROCRYPT '95*, volume 921 of *Lecture Notes in Computer Science*, pages 209–219. Springer Verlag, 1995.

[17] S. von Solms and D. Naccache. On blind signatures and perfect crimes. *Computer & Security*, 11(6):581–583, 1992.

Organization TC 3600 Bldg./Room KNOX
U. S. DEPARTMENT OF COMMERCE
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450
IF UNDELIVERABLE RETURN IN TEN DAYS

OFFICIAL BUSINESS

UNITED STATES POSTAGE
02 1A
0004205065
MAILED FROM ZI

AN EQUAL OPPORTUNITY EMPLOYER